

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

KAREN KRISE, et al.,

Plaintiffs,

v.

SEI/AARON'S, INC.  
a franchisee of Aaron's, Inc.  
doing business as  
Aaron's Sales and Leasing, et al.,

Defendants.

CIVIL ACTION FILE  
NO. 1:14-CV-1209-TWT

**OPINION AND ORDER**

The Plaintiffs Karen Krise, Corie Cason, Chauncey Robertson, Sr., and Jamie Robertson allege that the Defendant SEI/Aaron's, Inc. – a franchisee of Aaron's, Inc. – unlawfully accessed their computers from a remote location and collected private information stored therein. It is before the Court on the Defendant's Motion for Summary Judgment [Doc. 97], Motion to Exclude the Testimony of Micah Sherr [Doc. 104], and Motion to Exclude the Testimony of Michael Maschke [Doc. 111]. For the reasons set forth below the Defendant's Motion to Exclude the Testimony of Micah Sherr [Doc. 104] is GRANTED in part and DENIED in part; the Defendant's

Motion to Exclude the Testimony of Michael Maschke [Doc. 111] is DENIED; and the Defendant’s Motion for Summary Judgment [Doc. 97] is GRANTED.

## **I. Background**

The Defendant SEI/Aaron’s, Inc. (“SEI”) – a Georgia corporation with its headquarters in Atlanta, Georgia – is in the rent-to-own business.<sup>1</sup> Between 2010 and 2011, it operated approximately seventy franchise stores, which were located in Connecticut, Kentucky, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont.<sup>2</sup> From October 5, 2010 to December 27, 2011, the Defendant installed a software program – PC Rental Agent (“PCRA”) – on all computers it leased to its customers.<sup>3</sup> PCRA, which was owned by a company named DesignerWare, enabled the Defendant to “render a computer inoperable” by simply logging onto the DesignerWare website and placing a computer on “lockdown” mode.<sup>4</sup> Once the computer was locked, a customer could not use it and had to contact an SEI store to have the computer unlocked.<sup>5</sup> On August 8, 2011, DesignerWare

---

<sup>1</sup> Pls.’ Statement of Facts ¶ 21.

<sup>2</sup> Def.’s Statement of Facts ¶ 1.

<sup>3</sup> Id. ¶ 3.

<sup>4</sup> Id. ¶ 10.

<sup>5</sup> Id.

added a geolocation feature to PCRA.<sup>6</sup> This feature “directed the PCRA software installed on a computer to include the Wi-fi signals the computer picked up in its periodic reports.”<sup>7</sup> Finally, DesignerWare offered the “Detective Mode” feature on computers with PCRA installed.<sup>8</sup> Detective Mode could be remotely installed and activated, and once activated, it could capture keystrokes in addition to the content of the computer screen and clipboard.<sup>9</sup> Any data captured by Detective Mode would automatically be sent every two minutes to a designated email address.<sup>10</sup>

The Defendant states that it maintained a policy of informing customers during the lease closing that PCRA was installed on their computers, and that the software enabled SEI to track, monitor, and lock down the leased computers.<sup>11</sup> Moreover, according to the Defendant, each customer signed an Addendum to the lease

---

<sup>6</sup>        Id. ¶ 34.

<sup>7</sup>        Id. ¶ 35. It is undisputed that SEI never attempted to track any of the Plaintiffs’ computers using the geolocation feature. Id. ¶¶ 105, 143.

<sup>8</sup>        Id. ¶ 11.

<sup>9</sup>        Id. ¶ 12. It is undisputed that PCRA, by itself, could not capture this type of data. Id. ¶ 14.

<sup>10</sup>        Id. ¶ 12.

<sup>11</sup>        Id. ¶ 18.

agreement acknowledging that he or she was aware of the software's capabilities.<sup>12</sup>

The Defendant also contends that it retained ownership of each computer until a customer exercised one of two purchase options.<sup>13</sup> In adherence to SEI policy, the Defendant asserts that the general manager of each SEI store had the credentials to log onto the DesignerWare website and lock down a computer.<sup>14</sup> For Detective Mode, only the district managers and SEI's Director of Operational Support, Tennyson Cox, had the log in credentials to install and activate the feature.<sup>15</sup> The Defendant stopped using Detective Mode on May 6, 2011.<sup>16</sup> On or about January 23, 2012, the Defendant removed PCRA from all leased computers connected to the internet.<sup>17</sup>

The Plaintiffs Chauncey Robertson, Sr. and Jamie Robertson leased their laptop on October 7, 2010 from an SEI store in Meriden, Connecticut.<sup>18</sup> According to the

---

<sup>12</sup> Id. The Plaintiffs deny signing the Addendum. Pls.' Resp. to Def.'s Statement of Facts ¶ 19.

<sup>13</sup> Def.'s Statement of Facts ¶ 21.

<sup>14</sup> Id. ¶ 22.

<sup>15</sup> Id. ¶ 26.

<sup>16</sup> Id. ¶ 31.

<sup>17</sup> Id. ¶ 37.

<sup>18</sup> Id. ¶ 49.

Defendant, Ms. Robertson executed the lease documents, including the Addendum.<sup>19</sup> The Plaintiffs deny that Ms. Robertson signed the Addendum.<sup>20</sup> On November 9, 2010, SEI activated Detective Mode on the Robertsons' computer.<sup>21</sup> Detective Mode was deactivated on November 10, 2010.<sup>22</sup> The Defendant characterizes the activation as an error. It states that a different customer reported his computer as stolen, and SEI was attempting to locate that computer by activating Detective Mode.<sup>23</sup> The Defendant contends that the mix up occurred because the computers were the same brand with a similar or identical model number.<sup>24</sup> The Plaintiffs counter that the activation was not in error.<sup>25</sup> Beyond the Detective Mode activation, the Robertsons contend that their computer was slow and eventually returned the computer on June 27, 2011.<sup>26</sup>

---

<sup>19</sup> Id. ¶ 51.

<sup>20</sup> Pls.' Resp. to Def.'s Statement of Facts ¶ 51.

<sup>21</sup> Def.'s Statement of Facts ¶ 61.

<sup>22</sup> Id. ¶ 65.

<sup>23</sup> Id. ¶¶ 53, 61-62.

<sup>24</sup> Id. ¶ 62.

<sup>25</sup> Pls.' Resp. to Def.'s Statement of Facts ¶ 65.

<sup>26</sup> Def.'s Statement of Facts ¶¶ 70, 77.

The Plaintiff Corie Cason leased her computer on March 4, 2011, from an SEI store in Buffalo, New York.<sup>27</sup> The Defendant asserts that Cason executed both the computer lease agreement and the Addendum, but it does not possess either document.<sup>28</sup> The Plaintiffs deny that Cason signed the Addendum.<sup>29</sup> Similar to the Robertsons, Cason contends that her leased computer was “sluggish.”<sup>30</sup> Based on the computer’s allegedly slow speed, Cason brought it in for service in 2012 and 2014.<sup>31</sup> She eventually returned the computer to SEI in March of 2014.<sup>32</sup> The Defendant contends that, in 2011, only three months after she leased the computer, Cason learned about PCRA through a news article and the Plaintiffs’ counsel’s website.<sup>33</sup> Yet, she chose to keep the computer until 2014.<sup>34</sup> Cason testified that she learned about PCRA

---

<sup>27</sup> Id. ¶ 85.

<sup>28</sup> Id. ¶ 86.

<sup>29</sup> Pls.’ Resp. to Def.’s Statement of Facts ¶ 87.

<sup>30</sup> Def.’s Statement of Facts ¶ 90.

<sup>31</sup> Id. ¶¶ 96-97.

<sup>32</sup> Id. ¶ 100.

<sup>33</sup> Id. ¶¶ 91-92.

<sup>34</sup> Id. ¶ 94.

through a news article and website, but could not recall what date she learned about PCRA.<sup>35</sup>

The Plaintiff Karen Krise leased her computer on August 24, 2011, from an SEI store in Massena, New York.<sup>36</sup> The Defendant asserts that Krise signed the PCRA Addendum on the same day she leased her computer.<sup>37</sup> The Plaintiffs, however, dispute this account. Krise denies that she signed the Addendum at the time of the lease.<sup>38</sup> Soon after leasing the computer, Krise began to make late and/or partial lease payments.<sup>39</sup> Because of the late payments, on October 14, 2011, SEI placed Krise's computer in lockdown mode.<sup>40</sup> That same day, Krise made her lease payment and was given a code to unlock the computer.<sup>41</sup> Krise alleges that, on October 13, 2011, using the leased computer, she set up an E-bay auction that was scheduled for the next day.<sup>42</sup> She claims that once she unlocked her computer, all of her data had been deleted and

---

<sup>35</sup> Pls.' Resp. to Def.'s Statement of Facts ¶ 93.

<sup>36</sup> Def.'s Statement of Facts ¶ 106.

<sup>37</sup> Id. ¶ 107.

<sup>38</sup> Pls.' Resp. to Def.'s Statement of Facts ¶ 107.

<sup>39</sup> Def.'s Statement of Facts ¶¶ 110-16.

<sup>40</sup> Id. ¶ 119.

<sup>41</sup> Id. ¶ 120.

<sup>42</sup> Id. ¶ 117.

the computer had been restored to factory settings.<sup>43</sup> Because her computer data was deleted and she was unable to use her computer while on lockdown, Krise alleges that she lost potential E-bay bids.<sup>44</sup> Then, on October 15, 2011, Krise went on Herman Gerel's website, "webcamlawsuits.com."<sup>45</sup> There, she learned about PCRA and the litigation surrounding use of the software.<sup>46</sup> Despite the potential presence of the software, Krise kept the computer until December 19, 2011.<sup>47</sup> Krise, however, contends that between October and December she rarely used the computer and would cover the webcam with tape.<sup>48</sup>

On April 23, 2014, the Plaintiffs filed a class action complaint against SEI. They seek to represent a class of "(a) all persons who have purchased, leased, and/or rented ("Lease-Purchase" or "Lease-Purchased") from SEI personal computers on which PC Rental Agent had been installed without such persons' consent, and (b) all members of each such person's household."<sup>49</sup> The Plaintiffs allege that SEI did not

---

<sup>43</sup> Id. ¶ 121.

<sup>44</sup> Id. ¶ 124.

<sup>45</sup> Id. ¶ 131.

<sup>46</sup> Id.

<sup>47</sup> Id. ¶ 139.

<sup>48</sup> Pls.' Resp. to Def.'s Statement of Facts ¶ 134.

<sup>49</sup> Second Am. Compl. ¶ 1.

disclose to its customers that it installs PCRA on its leased computers or that it used Detective Mode to obtain data from the computers.<sup>50</sup> Furthermore, they allege that PCRA harmed the leased computers by, among other things, making them slow.<sup>51</sup> They allege five counts, including invasion of privacy; computer trespass, O.C.G.A. § 16-9-93(b); computer invasion of privacy, O.C.G.A. § 16-9-93(c); and violation of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2511.<sup>52</sup> The Defendant now moves for summary judgment on each of the Plaintiffs’ claims.<sup>53</sup>

## **II. Legal Standards**

### **A. Daubert Motion**

Federal Rule of Evidence 702 governs the admission of expert opinion testimony. Pursuant to that rule, before admitting expert testimony a court must consider: (1) whether the expert is competent to testify regarding the matters he intends to address; (2) whether the methodology used to reach his conclusions is sufficiently reliable; and (3) whether the testimony is relevant, in that it assists the jury

---

<sup>50</sup> Id. ¶ 3.

<sup>51</sup> See Pls.’ Resp. Br., at 31-32.

<sup>52</sup> Second Am. Compl. ¶¶ 51-74.

<sup>53</sup> [Doc. 97].

to understand the evidence or determine a fact in issue.<sup>54</sup> In ruling on the admissibility of expert testimony, “[t]he focus must be ‘solely’ on the expert’s ‘principles and methodology, not on the conclusions that they generate.’”<sup>55</sup> If the expert predicates his testimony on an assumption that is belied by the evidence, the expert’s testimony is properly excluded.<sup>56</sup> The party offering the expert's testimony has the burden to prove it is admissible by a preponderance of the evidence.<sup>57</sup>

## **B. Motion for Summary Judgment**

Summary judgment is appropriate only when the pleadings, depositions, and affidavits submitted by the parties show no genuine issue of material fact exists and that the movant is entitled to judgment as a matter of law.<sup>58</sup> The court should view the evidence and any inferences that may be drawn in the light most favorable to the

---

<sup>54</sup> Fed. R. Evid. 702; Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 589 (1993).

<sup>55</sup> KW Plastics v. United States Can Co., 131 F. Supp. 2d 1289, 1292 (M.D. Ala. 2001) (quoting Daubert, 509 U.S. at 594-95).

<sup>56</sup> Ferguson v. Bombardier Services Corp., 244 Fed Appx. 944, 949 (11th Cir. 2007).

<sup>57</sup> Allison v. McGhan Medical Corp., 184 F.3d 1300, 1306 (11th Cir. 1999).

<sup>58</sup> FED. R. CIV. P. 56(a).

nonmovant.<sup>59</sup> The party seeking summary judgment must first identify grounds to show the absence of a genuine issue of material fact.<sup>60</sup> The burden then shifts to the nonmovant, who must go beyond the pleadings and present affirmative evidence to show that a genuine issue of material fact does exist.<sup>61</sup> “A mere ‘scintilla’ of evidence supporting the opposing party’s position will not suffice; there must be a sufficient showing that the jury could reasonably find for that party.”<sup>62</sup>

### **III. Discussion**

#### **A. Daubert Motions**

##### **1. Micah Sherr**

The Defendant moves to exclude the testimony of the Plaintiffs’ expert Micah Sherr. The Defendant does not challenge Sherr’s qualifications. Instead, the Defendant contends that Sherr’s testimony fails to satisfy the relevance prong, because he did not apply his principles and methods reliably to the facts of the case. The Defendant asserts that Sherr’s opinions regarding the ECPA are unreliable because they are based on an incorrect legal standard. The ECPA is only applicable to electronic

---

<sup>59</sup> Adickes v. S.H. Kress & Co., 398 U.S. 144, 158-59 (1970).

<sup>60</sup> Celotex Corp. v. Catrett, 477 U.S. 317, 323-24 (1986).

<sup>61</sup> Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 257 (1986).

<sup>62</sup> Walker v. Darby, 911 F.2d 1573, 1577 (11th Cir. 1990).

communications that are intercepted, meaning acquired “contemporaneous with transmission.”<sup>63</sup> The Eleventh Circuit defines “contemporaneous with transmission” to mean the electronic communication is captured “in flight.”<sup>64</sup> The Defendant states that Sherr’s reports and testimony do not apply the “in flight” standard. Specifically, SEI argues that “Sherr opines that a communication can be ‘intercepted’ for purposes of the ECPA if it is captured ‘in close time proximity’ to transmission, rather than during transmission.”<sup>65</sup> In response, the Plaintiffs assert that Sherr is not creating a different legal standard, and that Sherr’s testimony should not be excluded merely because he did not use the phrase “in flight.”<sup>66</sup> They point out that Sherr testified that Detective Mode’s functions could capture electronic information contemporaneously with its transmission.<sup>67</sup>

The Court finds that the expert Sherr’s opinion should not be excluded. Some courts have concluded that receipt of the electronic communication “within a second”

---

<sup>63</sup>        United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003).

<sup>64</sup>        Id. at 1049-50.

<sup>65</sup>        Def.’s Mot. to Exclude Sherr, at 6-7.

<sup>66</sup>        Pls.’ Resp. to Def.’s Mot. to Exclude Sherr, at 3.

<sup>67</sup>        Id. at 2-3.

is contemporaneous.<sup>68</sup> But what qualifies as contemporaneous with transmission is “not so well-defined or beyond reasonable argument that th[e] issue[] should be effectively decided by a *Daubert* order.”<sup>69</sup> Sherr opined that Detective Mode’s keystroke feature is capable of intercepting communication “nearly at the instant the communication is transmitted over the network.”<sup>70</sup> He further noted that “[s]ince PCRA with Detective Mode continuously captures keystrokes as they occur, any and all typed communication will be intercepted at the time in which the user inputs the communication.”<sup>71</sup> Sherr’s opinions and testimony do not strike the Court as unreliable. They provide at least a reasonable argument as to what qualifies as contemporaneous in the context of Detective Mode. The Court therefore declines to exclude Sherr’s opinions and testimony regarding the contemporaneous interception of electronic communications. The issue of what constitutes a contemporaneous interception will be addressed in the context of the Defendant’s Motion for Summary Judgment.

---

<sup>68</sup>        United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010).

<sup>69</sup>        In re Southeastern Milk Litig., No. 2:08-MD-1000, 2010 WL 5102974, at \*2 (E.D. Tenn. Dec. 8, 2010).

<sup>70</sup>        Def.’s Mot. for Summ. J., Ex. M, Sherr Oct. 5, 2016 Expert Report ¶¶ 8-9.

<sup>71</sup>        Id. ¶ 6.

Next, the Defendant seeks to exclude Sherr's opinions related to the Plaintiffs' computer trespass claims. The Plaintiffs allege that the Defendant committed computer trespass under O.C.G.A. § 16-9-93(b). To commit a computer trespass under O.C.G.A. § 16-9-93(b), a person must use a computer with the knowledge that he or she is without authority to use it and with the intention of "[o]bstructing, interrupting, or in any way interfering with the use of a computer program or data."<sup>72</sup> In addition, the plaintiff's person or property must be damaged via the computer trespass.<sup>73</sup> The Plaintiffs here allege that the installation of PCRA constitutes a computer trespass because PCRA made the leased computers sluggish. In support of their allegations, the Plaintiffs rely on Sherr's opinions regarding PCRA's purported flaws. In his expert report, Sherr identified three alleged flaws – weakened security, memory leak, and data loss – which the Plaintiffs contend caused the alleged sluggishness.<sup>74</sup> The Defendant argues that Sherr's opinions regarding the purported flaws are speculative, because they are based on a limited review of the PCRA source code, not on an actual computer with PCRA installed. The Defendant also notes that Sherr's testimony fails to account for obvious alternative causes for the alleged damage.

---

<sup>72</sup> O.C.G.A. § 16-9-93(b)(2).

<sup>73</sup> Id. § 16-9-93(g).

<sup>74</sup> Def.'s Mot. for Summ. J., Ex. L, Sherr July 15, 2016 Expert Report ¶¶ 14, 24, 26.

The Court agrees with the Defendant. Sherr's opinions with regard to the speed of the computers are unsupported speculations that do not assist the trier of fact. In his report, Sherr opines that by removing various security features on the computer operating system, PCRA increased the likelihood of a malware infection.<sup>75</sup> And because malware may cause a computer to run slow, PCRA may be to blame for the alleged sluggishness.<sup>76</sup> For memory leak and data loss, Sherr opined that “[b]oth memory leaks and memory corruption can contribute to (1) the ‘sluggishness’ of a computer and (2) the stability of the software running on that computer,” and that he “found numerous instances in which PCRA can cause loss of user data.”<sup>77</sup> “For example, PCRA could cause the contents of an email that is being composed in an Internet browser to be permanently lost. Additionally, PCRA may cause additional data loss by preventing access to critical components of the operating system that are intended to help the user recover lost data.”<sup>78</sup> These equivocal statements with regard to the cause of the alleged computer damage do not assist the trier of fact to determine

---

<sup>75</sup> Id. ¶¶ 14-23.

<sup>76</sup> Sherr Dep., at 25-28.

<sup>77</sup> Def.'s Mot. for Summ. J., Ex. L, Sherr July 15, 2016 Expert Report ¶¶ 25-26.

<sup>78</sup> Id.

causation.<sup>79</sup> To assist the trier of fact, the evidence presented must be relevant. Federal Rule of Evidence 401 defines relevant evidence as having “any tendency to make a fact more or less probable than it would be without the evidence.”<sup>80</sup> Sherr’s consistent use of “may,” “can,” and “could” makes Sherr’s statements merely possible, not more probable.<sup>81</sup> A statement that something is merely possible “does not ‘logically advance a material aspect of [the Plaintiffs’] case.’”<sup>82</sup> Thus, the Court grants the Defendant’s Motion to Exclude Sherr’s opinions regarding computer performance.

## **2. Michael Maschke**

The Defendant seeks to exclude the opinions of the Plaintiffs’ expert, Michael Maschke. The Defendant asserts that Maschke’s opinions are unreliable, because they are based on cursory and unscientific examinations of computers with PCRA. However, the Court finds the Defendant’s Motion to be premature. The Plaintiffs do not rely on Maschke’s opinions in their response to the Defendant’s Motion for Summary Judgment. Moreover, the Plaintiffs state that they have not decided whether

---

<sup>79</sup> Bowers v. Norfolk Southern Corp., 537 F. Supp. 2d 1343, 1368 (M.D. Ga. 2007).

<sup>80</sup> FED. R. EVID. 401.

<sup>81</sup> Bowers, 537 F. Supp. 2d at 1368.

<sup>82</sup> Id. (quoting Allison v. McGhan Med. Corp., 184 F.3d 1300, 1312 (11th Cir. 1999)).

they will use the Maschke's testimony at trial.<sup>83</sup> The Court therefore denies without prejudice the Defendant's Motion to Exclude the Testimony of Michael Maschke.<sup>84</sup>

## B. Robertsons' Claims

### 1. Standing

The Defendant asserts that the Plaintiffs Chauncey Robertson, Sr. and Jamie Robertson do not have standing to allege any claims based on the Defendant's use of Detective Mode. The Robertsons were not originally part of the instant lawsuit. They were added as a party on June 18, 2014, when the Plaintiffs filed a First Amended Complaint.<sup>85</sup> In the original Complaint, none of the named Plaintiffs alleged that Detective Mode was installed on their computers. As a result, the Defendant contends that because "at least one named class representative must have Article III standing to raise each subclaim" in a Complaint, the Plaintiffs cannot amend their Complaint to add the Robertsons' claims based on Detective Mode.<sup>86</sup>

---

<sup>83</sup> Pls.' Resp. to Def.'s Mot. to Exclude Maschke, at 2-3.

<sup>84</sup> See, e.g., Johnson v. Allstate Ins. Co., No. 1:06-cv-14(WLS), 2006 WL 2617127, at \*1 (M.D. Ga. Sept. 12, 2006) (denying without prejudice a motion to exclude expert testimony because the expert testimony was not germane to the pending motion for summary judgment).

<sup>85</sup> [Doc. 31].

<sup>86</sup> Def.'s Mot. for Summ. J., at 7 (quoting Prado-Steiman v. Bush, 221 F.3d 1266, 1279-80 (11th Cir. 2000)).

The Court disagrees. The case the Defendant cites in support of its argument is distinguishable. In Wright v. Dougherty County, Georgia, the Eleventh Circuit held that because a plaintiff lacked standing to bring *any* claim against the defendant, the plaintiff “also lack[ed] standing to amend the complaint to consolidate with a party who may have standing.”<sup>87</sup> Here, the Defendant does not challenge the original Plaintiffs’ standing to assert claims based on the Defendant’s use of PCRA. And because the original Plaintiffs have standing to assert their original claims, the original Plaintiffs also have the right to seek leave to amend their Complaint to add additional plaintiffs. Indeed, the Plaintiffs sought leave, and the Court granted it.<sup>88</sup> The Court therefore concludes that the Robertsons have standing to assert all of their claims.

---

<sup>87</sup> Wright v. Dougherty Cnty., Ga., 358 F.3d 1352, 1356 (11th Cir. 2004).

<sup>88</sup> See FED. R. CIV. P. 15(a)(2) (“[A] party may amend its pleading only with the opposing party’s written consent or the court’s leave,” and “[t]he court should freely give leave when justice so requires.”).

## **2. Invasion of Privacy - Detective Mode**

In Count I of their Second Amended Complaint, the Plaintiffs assert an invasion of privacy/intrusion on seclusion claim. The Plaintiffs allege that the Defendant's activation of Detective Mode on the Robertsons' computer invaded the Robertsons' privacy. The Defendant contends that the Robertsons' invasion of privacy claim based on the Detective Mode activation is barred by the applicable statute of limitations.<sup>89</sup> For privacy torts, Georgia applies a two-year statute of limitations, and "the statute of limitation generally begins to run at the time damage caused by a tortious act occurs."<sup>90</sup> As noted above, Detective Mode was activated on the Robertsons' computer on November 9-10, 2010. Thus, the Robertsons' statute of limitations expired on November 10, 2012, which is, of course, well before the filing of the instant class action on April 23, 2014. Moreover, because no class actions were filed prior to November 10, 2012, no class action tolled the Robertsons' claim. As a result,

---

<sup>89</sup> Under Georgia choice of law, foreign statutes of limitations are procedural in nature. Thus, a federal court sitting in diversity applies the applicable Georgia statute of limitations and tolling provision. See Branch v. Sickert, No. 2:10-cv-128-RWS, 2011 WL 796783, at \*2 (N.D. Ga. Feb. 28, 2011) ("Georgia law generally regards foreign statutes of limitations as procedural and will apply its own statute of limitations." (citing Hudnall v. Kelly, 388 F. Supp. 1352, 1354 (N.D. Ga. 1975))).

<sup>90</sup> O.C.G.A. § 9-3-33; Rivell v. Private Health Care Sys., Inc., 887 F. Supp. 2d 1277, 1284-85 (S.D. Ga. 2012) (quoting Everhart v. Rich's, Inc., 229 Ga. 798, 801 (1972)).

the Robertsons' invasion of privacy of claim, insofar as it is based on the Defendant's activation of Detective Mode, is time barred.

### **3. Invasion of Privacy - PCRA**

The Plaintiffs also allege that the Defendant's installation of PCRA on the Robertsons' computer invaded the Robertsons' privacy. The Defendant, once again, asserts that the Robertsons' claim is time barred. The Robertsons returned their computer to SEI on June 27, 2011. As a result, any invasion of privacy claim had to be filed by June 27, 2013. However, the Plaintiffs contend that, pursuant to the rule of American Pipe & Construction Co. v. Utah,<sup>91</sup> the Robertsons' claim was tolled by a prior class action. On March 5, 2013, Gwendolyn Sneed filed a putative class action against SEI, alleging claims for invasion of privacy based on SEI's activation of Detective Mode and installation of PCRA.<sup>92</sup> Then, on May 20, 2014, Sneed voluntarily dismissed her case prior to the district court's ruling on class certification.<sup>93</sup> According to the Plaintiffs, the Sneed action tolled the Robertsons' invasion of privacy claim.

---

<sup>91</sup> 414 U.S. 538 (1974).

<sup>92</sup> Sneed v. SEI/Aaron's, Inc., No. 1:13-cv-00982-TWT (N.D. Ga.), [Doc. 1].

<sup>93</sup> Id. at [Doc. 44].

In American Pipe, the Supreme Court held that “the commencement of a class action suspends the applicable statute of limitations as to all asserted members of the class who would have been parties had the suit been permitted to continue as a class action.”<sup>94</sup> If and when class certification is denied, the limitations period begins to run.<sup>95</sup> The Defendant counters that the Robertsons’ claim cannot be tolled because the Sneed action was voluntarily dismissed. It is generally accepted that a voluntarily dismissed complaint does not toll the statute of limitations.<sup>96</sup> “This is because the law treats a voluntarily dismissed complaint as if it never had been filed.”<sup>97</sup> The question therefore becomes how the general rule regarding voluntarily dismissed complaints affects a subsequent class action based on the same conduct.

In arguing that the general rule is inapplicable, the Plaintiffs rely on Sawyer v. Atlas Heating and Sheet Metal Works, Inc.<sup>98</sup> There, the Seventh Circuit held that

---

<sup>94</sup>        American Pipe, 414 U.S. at 554.

<sup>95</sup>        Crown, Cork & Seal Co., Inc. v. Parker, 462 U.S. 345, 353-54 (1983).

<sup>96</sup>        See Weldon v. Electronic Data Sys., 138 F. App’x 136, 138 (11th Cir. 2005) (finding that a voluntarily dismissed complaint did not toll the statute of limitations); CHARLES ALAN WRIGHT & ARTHUR R. MILLER, 9 FED. PRAC. & PROC. CIV. § 2367 (3d ed.).

<sup>97</sup>        In re IndyMac Mortgage-Backed Securities Litig., 718 F. Supp. 2d 495, 504 (S.D.N.Y. 2010).

<sup>98</sup>        642 F.3d 560 (7th Cir. 2011).

“[t]olling lasts from the day a class claim is asserted until the day the suit is conclusively not a class action – which may be because the judge rules adversely to the plaintiff, or because the plaintiff reads the handwriting on the wall and decides not to throw good money after bad.”<sup>99</sup> Thus, the Seventh Circuit held that a voluntarily dismissed class action does toll the putative class members’ individual claims. The Seventh Circuit then answered an additional, more contested question: whether a successive class action that relies on American Pipe’s tolling principle may proceed as a class action when the prior class action complaint was voluntarily dismissed. In answering this question in the affirmative, the Seventh Circuit held that a successive class action is precluded by a prior class action only when a “court denies certification for a reason that would be equally applicable to any later suit – for example, that the supposed victims are too few to justify class litigation . . . then members of the asserted class are bound by that decision.”<sup>100</sup> But if the court denied certification in the first class action because the class representative was inappropriate, “then there is no basis for binding other members of the putative class, who have yet to receive a judicial decision on the question whether a class is certifiable under Rule 23.”<sup>101</sup>

---

<sup>99</sup>        Id. at 563.

<sup>100</sup>        Id. at 564.

<sup>101</sup>        Id.

The Eleventh Circuit disagrees with the Seventh Circuit's approach regarding prior class actions. In Ewing Industries Corp. v. Bob Wines Nursery, Inc., the Eleventh Circuit, citing Griffin v. Singletary, held that a prior class action that was dismissed because of an inadequate class representative – and not because of a defect in the class itself – did not toll the statute of limitations for a subsequent class action.<sup>102</sup> Thus, unlike the Seventh Circuit in Sawyer, the Eleventh Circuit found that every proposed class is *not* entitled to at least one attempt at class certification.<sup>103</sup> The court noted that its holding prevented “the potential for multiple rounds of litigation as the class seeks an adequate class representative.”<sup>104</sup> In accordance with the principle laid out in Ewing Industries, the Court finds that the Sneed action did not toll the Robertsons’ class claim for invasion of privacy. If a named plaintiff’s voluntarily dismissal of a class action tolled all future class action claims, the potential for “piggybacked” class actions arises. The initial class counsel could determine a class representative is inadequate and preemptively seek a voluntarily dismissal. Then, the class action could be filed again and again, with the hopes of finding an adequate representative. The Eleventh Circuit warned against “adopt[ing] any rule that has the

---

<sup>102</sup> 795 F.3d 1324, 1328 (11th Cir. 2015).

<sup>103</sup> Id. at 1326.

<sup>104</sup> Id. at 1328.

potential for prolonging litigation about class representation even further.”<sup>105</sup> The Court will follow the Eleventh Circuit’s warning: the Robertsons may not pursue their invasion of privacy claim as a class claim.

Nevertheless, the Court finds that the Robertsons may pursue their invasion of privacy claim as an individual claim. Relying on In re IndyMac Mortgage-Backed Securities Litigation, the Defendant argues that the Robertsons’ individual invasion of privacy claim should be dismissed. In that case, the plaintiffs argued that their claims were tolled by a prior class action complaint.<sup>106</sup> But the Southern District of New York held that the American Pipe rule does not apply where the initial complaint was dismissed voluntarily.<sup>107</sup> The court stated that because a voluntarily dismissed complaint is treated as if it was never filed, the initial complaint cannot toll the plaintiffs’ claims.<sup>108</sup> It is unclear to the Court, however, whether the In re IndyMac court was referring to the plaintiffs’ class claims or individual claims. The court’s opinion does not clearly delineate between the two. Even so, it seems rather harsh to find a putative class member’s individual claims are not tolled based on the whims of

---

<sup>105</sup> Id. (quoting Griffin v. Singletary, 17 F.3d 356, 359 (11th Cir. 1994)).

<sup>106</sup> In re IndyMac Mortgage-Backed Secs. Litig., 718 F. Supp. 2d 495, 504 (S.D.N.Y. 2010).

<sup>107</sup> Id. at 505.

<sup>108</sup> Id. at 504-05.

the class representative. As a result, the Court finds that the American Pipe rule is applicable to the Robertsons' individual invasion of privacy claim based on the Defendant's use of PCRA.

Next, the Defendant argues that the Robertsons' PCRA invasion of privacy claim fails because no private data was captured. Before the Court can address this issue, however, it must determine whether Georgia law is applicable to the Robertsons' invasion of privacy claim. The Defendant contends that Connecticut law should apply to the Plaintiffs' claim. Though not completely clear to the Court, the Plaintiffs appear to assert that Georgia law should apply.<sup>109</sup> A federal court sitting in diversity applies the choice of law rules of the forum state to determine which law applies.<sup>110</sup> Therefore, the Georgia choice of law rules apply here. Georgia follows the doctrine of *lex loci delicti*:<sup>111</sup>

The general rule is that the place of the wrong, the *locus delicti*, is the place where the injury was suffered rather than the place where the act was committed, or, as it is sometimes more generally put, it is the place

---

<sup>109</sup> The Plaintiffs specifically concede that New York law applies to the Plaintiffs Cason's and Krise's invasion of privacy claims. The Plaintiffs fail to note whether they agree with the Defendant's choice of law analysis with regard to the Robertsons' claim. See Pls.' Resp. Br., at 34 n.8.

<sup>110</sup> Klaxon Co. v. Stentor Elec. Mfg. Co., 313 U.S. 487, 496 (1941).

<sup>111</sup> Brenner v. Future Graphics, LLC, 258 F.R.D. 561, 571 (N.D. Ga. 2007).

where the last event necessary to make an actor liable for the alleged tort takes place.<sup>112</sup>

Thus, the substantive law of the jurisdiction where each Plaintiff suffered harm would apply to their claims. However, Georgia choice of law doctrine applies a unique exception to the *lex loci delicti* doctrine. When a harm is suffered out of state, the application of that state's laws "is limited to statutes and decisions construing those statutes."<sup>113</sup> If no statute is relevant, Georgia common law applies to the parties' claims.<sup>114</sup>

Nevertheless, Georgia common law will not apply if its application is inconsistent with due process. To determine whether the application of Georgia law to the Plaintiffs' claim is consistent with due process, "the court must analyze whether the State of Georgia has 'significant contact or significant aggregation of contacts to the claims asserted by each . . . [Plaintiff], contacts creating state interests, in order to ensure that the choice of Georgia law is not arbitrary or unfair.'"<sup>115</sup> Here, the

---

<sup>112</sup> Id. (quoting Risdon Enters., Inc. v. Colemill Enters., Inc., 172 Ga. App. 902, 903 (1984)).

<sup>113</sup> In re Tri-State Crematory Litig., 215 F.R.D. 660, 667 (N.D. Ga. 2003) (quoting Frank Briscoe Co., Inc. v. Georgia Sprinkler Co. Inc., 713 F.2d 1500, 1503 (11th Cir. 1983)).

<sup>114</sup> Brenner, 258 F.R.D. at 571.

<sup>115</sup> Id. (quoting Phillips Petroleum Co. v. Shutts, 472 U.S. 797, 821-22 (1985)).

Defendant SEI is a Georgia corporation with its principal place of business in Atlanta, Georgia. SEI purchased PCRA from its Atlanta office and made payments for the spyware from its Atlanta office.<sup>116</sup> But these are the only contacts to the state of Georgia. The Robertsons, who live in Connecticut, leased their computer from an SEI store in Connecticut. PCRA was installed on their leased computer at the Connecticut store, and any information gathered through PCRA would have been sent to an SEI employee at the Connecticut store. Finally, the Robertsons do not allege that they used their computer outside of the state of Connecticut.<sup>117</sup> As a result, the Court finds that Connecticut law should apply to the Robertsons' invasion of privacy claim.

Connecticut follows the Restatement (Second) of Torts' definition of intrusion upon seclusion: "intentionally intrud[ing], physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person."<sup>118</sup> The Defendant contends that the Robertsons' claim fails because PCRA – without Detective Mode installed and

---

<sup>116</sup> Pls.' Resp. Br., Ex. D.

<sup>117</sup> Def.'s Statement of Facts ¶ 83.

<sup>118</sup> Tedeschi v. Kason Credit Corp., No. 3:10cv00612 DJS, 2014 WL 1491173, at \*6 (D. Conn. April 15, 2014) (quoting RESTATEMENT (SECOND) OF TORTS § 652B (1977)); see also Goodrich v. Waterbury Republican-Am., Inc., 188 Conn. 107, 128 (1982).

activated – was incapable of collecting private information.<sup>119</sup> Rather, PCRA was only capable of capturing the IP address of the computer, which, according to the Defendant, is not highly offensive to a reasonable person. In response, the Plaintiffs argue that mere installation of PCRA is offensive to a reasonable person, because the Defendant was capable of installing Detective Mode through PCRA. They cite Koeppel v. Spiers in support of their argument.

In Koeppel, the Iowa Supreme Court addressed the question of “whether the harm sought to be remedied by the [intrusion upon seclusion] tort is caused by accessing information from the plaintiff in a private place or by placing mechanisms in a private place that are capable of doing so at the hand of the defendant.”<sup>120</sup> After a review of the relevant case law, the Koeppel court held that placing a device into private place that is capable of capturing private information is sufficient to state an intrusion upon seclusion claim.<sup>121</sup>

Based on a review of Connecticut case law, it does not appear that the Connecticut courts have weighed in on the issue. Nevertheless, the Court finds that the instant case is distinguishable from the circumstances in Koeppel. In Koeppel, the

---

<sup>119</sup> Def.’s Statement of Facts ¶ 14; Kelly Dep., at 40-46, 53, 65.

<sup>120</sup> Koeppel v. Speirs, 808 N.W. 2d 177, 184 (Iowa 2011).

<sup>121</sup> Id. at 185-86.

plaintiff brought suit against her employer after it was discovered that the employer installed a hidden camera in a workplace bathroom.<sup>122</sup> The employer contended that the plaintiff could not assert an invasion of privacy claim, because the camera never actually worked.<sup>123</sup> But the plaintiff submitted evidence that the camera was potentially capable of working when a fresh battery was in place.<sup>124</sup> The court held that because there was evidence that the camera was potentially capable of working, the plaintiff's claim could survive summary judgment.<sup>125</sup>

Here, the parties do not dispute that PCRA was incapable of capturing any private information. The Defendant needed to separately install and activate Detective Mode in order to potentially capture private information. The Court finds that this fact differentiates the instant case from the cases cited by the Plaintiffs. Those cases all involve circumstances where a person was subjected to a functioning recording device.<sup>126</sup> Outside of the two days Detective Mode was installed on the Robertsons'

---

<sup>122</sup> Id. at 178-79.

<sup>123</sup> Id. at 185.

<sup>124</sup> Id.

<sup>125</sup> Id.

<sup>126</sup> See, e.g., Amati v. City of Woodstock, Ill., 829 F. Supp. 998, 1010 (N.D. Ill. 1993) (finding that the placing of a recording device to capture private conversations is sufficient to assert an intrusion upon seclusion claim, even if the

computer, the Robertsons' computer was only installed with PCRA. Because PCRA was incapable of capturing private information, the Robertsons' intrusion upon seclusion claim cannot survive. The Court therefore grants the Defendant's Motion for Summary Judgment with regard to the Robertsons' invasion of privacy claim.

#### **4. Georgia Computer Systems Protection Act**

The Georgia Computer Systems Protection Act ("GCSPA") prohibits, *inter alia*, "computer trespass" and "computer invasion of privacy."<sup>127</sup> "Any person whose property or person is injured by reason of a violation" of the GCSPA may bring an action for damages.<sup>128</sup> The Robertsons allege that the installation of PCRA constitutes both a computer trespass and a computer invasion of privacy. The GCSPA does not apply extraterritorially.<sup>129</sup> Thus, in order to assert a claim under the GCSPA, a plaintiff's claim must have a sufficient connection to Georgia. The Defendant argues that none of the alleged injuries or unlawful acts took place in Georgia. It points to the following facts. The Robertsons, who are residents of Connecticut, leased their

---

defendant failed to listen to the private conversations).

<sup>127</sup> O.C.G.A. § 16-9-93.

<sup>128</sup> Id. § 16-9-93(g)(1).

<sup>129</sup> Peterson v. Aaron's, Inc., 108 F. Supp. 3d 1352, 1354 (N.D. Ga. 2015) (noting that "no part of the GCSPA indicates that it applies extra-territorially").

computer from an SEI store in Meriden, Connecticut.<sup>130</sup> PCRA was installed on the Robertsons' computer by an SEI employee at the Meriden store.<sup>131</sup> The Robertsons never used their computer outside of the state of Connecticut.<sup>132</sup> Any data received through PCRA was routed through a DesignerWare server in Pennsylvania and was emailed to SEI employees in Connecticut.<sup>133</sup> The employee who activated Detective Mode on the Robertsons' computer was located in Connecticut.<sup>134</sup>

According to the Defendant, this case is very similar to Peterson v. Aaron's, Inc.<sup>135</sup> In Peterson, this Court held that the plaintiffs could not assert a claim under the GCSPA because none of the alleged injuries or illegal conduct occurred in Georgia.<sup>136</sup> There, the plaintiffs, who were residents of Colorado and Oklahoma, leased a computer from a Montana-based franchisee store located in Colorado.<sup>137</sup> In response,

---

<sup>130</sup> Def.'s Statement of Facts ¶ 49.

<sup>131</sup> Id.

<sup>132</sup> Jamie Robertson Dep., at 71; Pls.' Resp. to Def.'s Statement of Facts ¶ 83.

<sup>133</sup> Kelly Dep., at 8, 82-84.

<sup>134</sup> Debrosse Aff. ¶ 16.

<sup>135</sup> 108 F. Supp. 3d 1352 (N.D. Ga. 2015).

<sup>136</sup> Id. at 1354-55.

<sup>137</sup> Id.

the Plaintiffs point out a few differences between Peterson and the instant action. First, SEI is a Georgia-based franchisee. Second, SEI purchased PCRA from its Atlanta office and made payments for the spyware from the Atlanta office. Third, the Plaintiffs allege that SEI's employees used "Aarons.com" email addresses for the installation and operation of PCRA, and they point out that the Aaron's email server is located in Atlanta.<sup>138</sup>

Despite SEI's connections to Georgia, the Court finds that the Plaintiffs cannot bring a claim under the GCSPA. To be sure, the instant case is a closer call than the Peterson case. Nevertheless, all of the alleged injuries and illegal conduct occurred outside the state of Georgia. The only allegation of illegal conduct that touches Georgia is contradicted by the evidence. The Plaintiffs allege that the Defendant installed PCRA through its employees' Aarons.com email addresses. But, according to the DesignerWare instruction manual, the computer does not connect to the internet until the installation process is complete.<sup>139</sup> Moreover, an SEI employee testified that PCRA was installed using a disk or thumb drive, not over the internet.<sup>140</sup> It was only

---

<sup>138</sup> Pls.' Resp. Br., at 20.

<sup>139</sup> Kelly Dep., Ex. 5, at 184.

<sup>140</sup> Cox Dep., at 51-53.

after PCRA was successfully installed and connected to the internet that an email would be sent to an SEI employee confirming the installation of PCRA.<sup>141</sup>

The Plaintiffs also argue that SEI's payments to DesignerWare from its Georgia office are sufficient contacts to Georgia. They cite the venue provision of the GCSPA in support of their contention. The venue provision states: "any violation of this article shall be considered to have been committed . . . (3) in any county in which any act was performed in furtherance of any transaction which violated this article[.]"<sup>142</sup> But, as the Defendant points out, this venue provision is only for the purpose of determining venue. Where, as here, all of the allegedly unlawful acts and injuries occurred outside the state of Georgia, the Court is unconvinced a plaintiff should be able to bring a claim under the GCSPA. Accordingly, the Defendant's Motion for Summary Judgment with regard to the Robertsons' GCSPA claim should be granted.

## **5. Violation of the Electronic Communications Privacy Act**

The Robertsons assert claims under 18 U.S.C. § 2511(1)(a)(c) and (d) of the Electronic Communications Protection Act ("ECPA"). As previously discussed, the ECPA imposes criminal and civil liability on any person who "intentionally intercepts

---

<sup>141</sup> Cason Dep., Ex. 1, at 1.

<sup>142</sup> O.C.G.A. § 16-9-94(3).

. . . any wire, oral or electronic communication.”<sup>143</sup> The ECPA also imposes liability on any person who “intentionally discloses” or “intentionally uses” the contents of an electronic communication if that person knows, or has reason to know, that the communication was intercepted in violation of the Act.<sup>144</sup> Therefore, in order to assert a claim under the ECPA, a plaintiff must prove that his or her communication was “intercepted.” The Eleventh Circuit has adopted a narrow reading of the term intercept in the context of electronic communications. Specifically, to prove an interception occurred, the electronic communications must have been acquired “contemporaneously with their transmission.”<sup>145</sup> Electronic communications are not intercepted under the ECPA if they are retrieved from storage.<sup>146</sup> In United States v. Steiger, for example, the Eleventh Circuit held that a computer hacker had not “obtained [information] through contemporaneous acquisition of electronic communications while in flight. Rather, the evidence show[ed] that the source used

---

<sup>143</sup> 18 U.S.C. § 2511(1)(a).

<sup>144</sup> Id. § 2511(1)(c), (d).

<sup>145</sup> United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003).

<sup>146</sup> Id.

a Trojan Horse virus that enabled him to access and download information on . . . [the] personal computer.”<sup>147</sup>

What qualifies as a contemporaneous interception is hotly disputed in most ECPA cases. This case is no different. Detective Mode is capable of capturing four different kinds of data from a computer: screen shots, clipboard content, key strokes, and web camera images and/or videos.<sup>148</sup> But both parties specifically focus on screenshots and keystrokes in their briefs and expert reports. The Defendant contends that the Plaintiffs cannot prove a contemporaneous interception occurred, because Detective Mode cannot capture communications while they are “in flight.” The Defendant’s expert, Professor Patrick McDaniel, concluded that Detective Mode “collects data from memory where it is stored locally on the machine.”<sup>149</sup> For example, “any data collected from the keyboard would not be captured simultaneous with transmission because it would be collected before it was sent.”<sup>150</sup> Professor McDaniel also noted that common tools for capturing data in flight – wire tapping, network data

---

<sup>147</sup> Id. at 1050.

<sup>148</sup> Def.’s Mot. for Summ. J., Ex. J(1), McDaniel May 11, 2016 Expert Report, at 13.

<sup>149</sup> Id.

<sup>150</sup> Id. at 15.

packeting sniffing, and packet capture – were not contained within the PCRA software.<sup>151</sup>

In response, the Plaintiffs cite their expert, Micah Sherr, who opined that PCRA is capable of capturing information simultaneously with its transmission. Sherr asserted that “Screenshot interceptions capture the contents of the user’s display the instant the screenshot was taken.”<sup>152</sup> Moreover, Sherr noted that PCRA captures keystrokes “as they occur, and hence any typed form of communication will be intercepted at the time at which the user inputs the communication.”<sup>153</sup> In a deposition, however, Sherr testified that PCRA captures information “[i]n close proximity” or “near in time” to its transmission.<sup>154</sup> This “near in time” capture happens at the “endpoints,” meaning at the local machine, not over the network.<sup>155</sup> For example, when PCRA takes a screenshot, PCRA can capture an image of a communication from

---

<sup>151</sup> Id.

<sup>152</sup> Def.’s Mot. for Summ. J., Ex. K, Sherr Expert Report, at 12.

<sup>153</sup> Id.

<sup>154</sup> Sherr Dep., at 80.

<sup>155</sup> Id. at 82.

one computer to another very soon after the communication has arrived at the recipient's computer.<sup>156</sup>

The issue, therefore, is whether PCRA's "near in time" capabilities constitute an interception under the PCRA. For its keystroke function, the Court finds PCRA does not "intercept" within the meaning of the ECPA. Based on the evidence put forth, it is clear that the keystroke function records typed-letters before they are transmitted, and thus it is only capturing the transmissions between the keyboard and the computer. Several courts have found that such keystroke functions are not capturing "electronic communications" that affect commerce.<sup>157</sup>

Detective Mode's screenshot function presents a more difficult question. Few courts have examined screenshot technology under the ECPA. Nevertheless, the Plaintiffs contend that Shefts v. Petrakis supports their argument that a screenshot that captures an image of a communication on a computer is contemporaneously copying

---

<sup>156</sup> Id. at 15.

<sup>157</sup> See United States v. Barrington, 648 F.3d 1178, 1202 (11th Cir. 2011) ("[U]se of a keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce."); Rene v. G.F. Fishers, Inc., 817 F. Supp. 2d 1090, 1094 (S.D. Ind. 2011) (agreeing with Barrington and holding that a keylogger intercepted keystrokes that were not electronic communications that affect interstate commerce).

the communication as it is transmitted. In Shefts, the plaintiff alleged that the defendants intercepted messages from his web-based email account by using a software called SpectorPro.<sup>158</sup> Similar to Detective Mode, SpectorPro operated by taking images of the user's activities on the computer.<sup>159</sup> The Shefts court held that the screen-captures constituted an interception under the ECPA.<sup>160</sup> It found that "any emails sent by Plaintiff on his Yahoo! account via his desktop computer would have been captured by SpectorPro *as they were transmitted* to Yahoo! via the internet."<sup>161</sup>

The Court, however, finds that SpectorPro is distinguishable from PCRA's Detective Mode. According to the Shefts court, SpectorPro was "always on," meaning it was constantly capturing screenshots.<sup>162</sup> Therefore – by default – it "capture[d] all communications simultaneously with their transmission."<sup>163</sup> But Detective Mode's screen-capture function was not always running. Instead, according to the Plaintiffs'

---

<sup>158</sup> Shefts v. Petrakis, No. 10-cv-1104, 2012 WL 4049484, at \*8 (C.D. Ill. Sept. 13, 2012).

<sup>159</sup> Id.

<sup>160</sup> Id. at \*9.

<sup>161</sup> Id. (emphasis in original).

<sup>162</sup> Id. at \*11 n.25.

<sup>163</sup> Id.

expert, it took screenshots every two minutes.<sup>164</sup> This means that Detective Mode did not automatically capture all communications simultaneously with their transmission. In fact, Detective Mode's screen-capture function is more akin to a different intercepting device discussed in Shefts. Specifically, the Shefts court found that "where the allegedly intercepting device operates only intermittently (rather than continuously, as in the SpectorPro instance), the amount of time between the transmission and interception by the spy is not the primary determining factor, but rather the fact that interception was automatically triggered by transmission or reception."<sup>165</sup> The court went on to find that because the intercepting device at issue "did not acquire the text messages as they were transmitted to or from Plaintiff, but acquired them from the Blackberry at predetermined intervals," it could not find that the device intercepted the messages under the ECPA.<sup>166</sup> Here, Detective Mode's screen-capture function is not triggered by the transmission or reception of electronic communications. Instead, it took a screenshot at predetermined intervals. Even if the Plaintiffs can show that a screenshot or two occurred in close proximity to an electronic communication, that does not mean the screenshot captured the

---

<sup>164</sup> Def.'s Mot. for Summ. J., Ex. K, Sherr Expert Report, at 12.

<sup>165</sup> Shefts, 2012 WL 4049484, at \*11.

<sup>166</sup> Id.

communication simultaneously with its transmission. Indeed, there is no evidence to demonstrate that a screenshot was ever triggered by a communication. As a result, the Court finds that Detective Mode's screenshot function did not intercept the Robertsons' electronic communications under the ECPA. The Defendant's Motion for Summary Judgment with regard to the Plaintiffs' ECPA claim is granted.

### **C. Cason's and Krise's Claims**

The Plaintiffs Corie Cason and Karen Krise allege both invasion of privacy and violation of the GCSPA. In their Response Brief, the Plaintiffs agreed with the Defendant's choice of law analysis and stated that Cason's and Krise's common law invasion of privacy claims should be dismissed.<sup>167</sup> Accordingly, the Defendant's Motion for Summary Judgment regarding the Plaintiffs Cason's and Krise's common law invasion of privacy claims is granted. As for Cason's and Krise's GCPSA claims, the Court reaches the same conclusion as it did with regard to the Robertsons' GCPSA claim. The Plaintiff Cason leased her computer from an SEI store in Buffalo, New York and never took the computer to Georgia.<sup>168</sup> PCRA was installed on her computer at the Buffalo store.<sup>169</sup> Detective Mode was never installed on Cason's computer and

---

<sup>167</sup> Pls.' Resp. Br., at 34 n.8.

<sup>168</sup> Def.'s Statement of Facts ¶ 85; Cason Dep., at 111-12.

<sup>169</sup> Def.'s Statement of Facts ¶ 85.

any information gathered from PCRA would have been emailed to a Buffalo store employee.<sup>170</sup> Similarly, the Plaintiff Krise leased her computer from a store in Massena, New York.<sup>171</sup> PCRA was installed on her computer at the time of the lease.<sup>172</sup> Krise does not allege that she ever took the computer to Georgia.<sup>173</sup> It is undisputed that Detective Mode was never installed on Krise's computer, and any information gathered through PCRA would have been sent to an employee at the Massena store.<sup>174</sup> Moreover, both lockdowns of the Plaintiff Krise's computer were executed by employees at the Massena store.<sup>175</sup> As the Court explained above, it is unwilling to allow the Plaintiffs' GCSPA claims to move forward when none of the alleged illegal conduct and injuries occurred in Georgia. The Defendant's Motion for Summary Judgment is granted as to the Plaintiffs Cason's and Krise's GCSPA claims.<sup>176</sup>

---

<sup>170</sup> Id. ¶ 104.

<sup>171</sup> Id. ¶ 106.

<sup>172</sup> Id.

<sup>173</sup> Krise Dep., at 138.

<sup>174</sup> Def.'s Statement of Facts ¶¶ 142-43.

<sup>175</sup> Cox Dep., at 51-53; Hunt Aff. ¶¶ 14-15.

<sup>176</sup> The Defendant also raises the issue of spoliation, asserting that the Plaintiffs Cason's and Krise's claims should be dismissed under Federal Rule of Civil

#### **IV. Conclusion**

For these reasons, the Defendant's Motion to Exclude the Testimony of Micah Sherr [Doc. 104] is GRANTED in part and DENIED in part; the Defendant's Motion to Exclude the Testimony of Michael Maschke [Doc. 111] is DENIED; and the Defendant's Motion for Summary Judgment [Doc. 97] is GRANTED.

---

Procedure 37. See Def.'s Mot. for Summ. J., at 48-50, 56-57. Because the Court is granting the Defendant's Motion for Summary Judgment as to all of Cason's and Krise's claims, it will not address the Defendant's spoliation allegations. The Defendant may bring a motion for sanctions based on the alleged spoliation if it wishes.

SO ORDERED, this 18 day of August, 2017.

/s/Thomas W. Thrash  
**THOMAS W. THRASH, JR.**  
United States District Judge